Math 357
Exam 03

2024–04–30 (T)

Your name: ________________________________

Honor pledge:

Instructions

1. In the space above, please legibly write your name and the Rice Honor Pledge, then sign.
2. Full time for this exam is exactly three hours. No resources are allowed.
3. Your reasoning—correctness and clarity—is more important than your "answer".
4. If you think there is ambiguity or error in an exercise, then briefly (!) write your understanding of the exercise and any additional hypotheses you are making, then proceed.

This exam is an imperfect measure of my understanding at a particular point in time. It is not a measure of who I am or who I will be.

Exercise	Total	(a)	(b)	(c)	(d)
Part 1					
1	/4	/4	/4	/4	/4
2	/4	/4	/4	/4	/4
3	/4	/4	/4	/4	
4	/4	/4	/4	/4	/4
Total	/16				
Part 2					
5	/4	/4	/4	/4	
6	/4	/4	/4	/4	/4
7	/4	/4	/4	/4	/4
8	/4	/4	/4	/4	/4
Total	/16				

Exercise 1

Let R be a commutative ring with a multiplicative identity $1_R \neq 0_R$, and let $I \subseteq R$.

(a) Define what it means for I to be (i) an ideal, (ii) a prime ideal, and (iii) a maximal ideal.

(b) Let I be an ideal of R. Prove that if I is maximal, then I is prime. (*Hint:* Use quotient rings.)

(c) Give an example to show that the converse to the statement in part (b) is false, in general. That is, give an example of a prime ideal that is not maximal.

(d) For each $i \in \mathbf{Z}_{>0}$, let I_i be an ideal of R such that $I_1 \subseteq I_2 \subseteq \ldots$. Prove that $I = \cup_{i \in \mathbf{Z}_{>0}} I_i$ is an ideal of R.

Solution: Part (a): Let $I \subseteq R$. I is an **ideal** of R if it is a subring of R and closed under multiplication by elements of R. This is equivalent to the following three conditions:

(i) Nonempty: $0_R \in I$.

(ii) Closed under $+$: For all $a_1, a_2 \in I$, $a_1 + a_2 \in I$.

(iii) Strongly closed under $\times$: For all $a \in I$, for all $r \in R$, $ra \in I$.

I is a **prime ideal** of R if it satisfies the following two conditions:

(i) I is a proper ideal of R (that is, $I \neq R$).

(ii) For all $r_1, r_2 \in R$, if $r_1 r_2 \in I$, then $r_1 \in I$ or $r_2 \in I$.

I is a **maximal ideal** of R if it satisfies the following two conditions:

(i) I is a proper ideal of R.

(ii) For all ideals J of R, if $I \subseteq J$, then either $J = I$ or $J = R$.

Part (b): Let $I \subseteq R$ be an ideal. Recall that I is maximal if and only if R/I is a field, and I is prime if and only if R/I is an integral domain. Also recall that a field is an integral domain. Thus

$$I \text{ maximal} \quad \Leftrightarrow \quad R/I \text{ a field} \quad \Rightarrow \quad R/I \text{ an integral domain} \quad \Leftrightarrow \quad I \text{ prime}$$

Part (c): Consider the ideal (0) in $\mathbf{Z}$. Because $\mathbf{Z}$ is an integral domain, (0) is a prime ideal. Because $\mathbf{Z}$ is not a field, (0) is not a maximal ideal. We can prove these assertions either by using the quotient $\mathbf{Z}/(0) \cong \mathbf{Z}$ (see our response to part (b)) or by using the definitions directly on the ideal (0) in $\mathbf{Z}$. For example, in the latter approach, let $a, b \in \mathbf{Z}$ such that $ab \in (0)$. This is equivalent to $ab = 0$. Because $\mathbf{Z}$ is an integral domain, this implies that either $a = 0$, equivalent to $a \in (0)$; or $b = 0$, equivalent to $b \in (0)$. Thus by definition, the ideal (0) is prime. (0) is contained in every ideal (n) of $\mathbf{Z}$, which is nonzero if $n \neq 0$ and proper if $n \neq \pm 1$. Thus the ideal (0) is not maximal.

As another example, let R be an integral domain that is not a field (for example, $R = \mathbf{Z}$ or $R = K[s]$ for K a field and s an indeteminate), let t be an indeterminate, and consider the ideal (t) in $R[t]$. Then $R[t]/(t) \cong R$ is an integral domain but not a field, so the ideal (t) is prime but not maximal.

Part (d): We verify that $\cup_{i \in \mathbf{Z}_{>0}} I_i$ satisfies the three axioms of an ideal that we listed in our response to part (a).

1. Nonempty. By hypothesis, for any (in fact, for all) $i \in \mathbf{Z}_{>0}$, I_i is an ideal of R, so $0_R \in I_i$. Hence $0_R \in \cup_{i \in \mathbf{Z}_{>0}} I_i$.

2. Closed under $+$. Let $r_1, r_2 \in \cup_{i \in \mathbf{Z}_{>0}} I_i$. Then there exist indices $i_1, i_2 \in \mathbf{Z}_{>0}$ such that $r_1 \in I_{i_1}$ and $r_2 \in I_{i_2}$. Without loss of generality, suppose that $i_1 \leqslant i_2$. By hypothesis, $I_1 \subseteq I_2 \subseteq \ldots$, so $I_{i_1} \subseteq I_{i_2}$, and hence $r_1, r_2 \in I_{i_2}$. By hypothesis, I_{i_2} is an ideal, so $r_1 + r_2 \in I_{i_2} \subseteq \cup_{i \in \mathbf{Z}_{>0}} I_i$.

3. Strongly closed under $\times$. Let $a \in \cup_{i \in \mathbf{Z}_{>0}} I_i$, and let $r \in R$. Then there exists some index $i_0 \in \mathbf{Z}_{>0}$ such that $a \in I_{i_0}$. By hypothesis, I_{i_0} is an ideal, so $ra \in I_{i_0} \subseteq \cup_{i \in \mathbf{Z}_{>0}} I_i$.

Exercise 2

(a) Define (i) integral domain, (ii) principal ideal domain, and (iii) field.

(b) Clearly present the logical implications among the following seven algebraic structures (no proof required):

> abelian group, euclidean domain (ED), field, integral domain (ID), principal ideal domain (PID), ring, unique factorization domain (UFD)

(c) Let R be a PID, and let $I \subseteq R$ be a prime ideal such that $I \neq (0_R)$. Prove that I is maximal.

(d) Now let R be a commutative ring, and let t be an indeterminate. Prove that the polynomial ring $R[t]$ is a PID if and only if R is a field.

Solution: Part (a): Let R be a ring. R is an **integral domain** if it is commutative, has a multiplicative identity $1_R \neq 0_R$, and has no zero divisors (that is, no elements $r_1, r_2 \in R - \{0\}$ such that $r_1 r_2 = 0_R$). R is a **field** if it is an integral domain such that every nonzero element is a unit (that is, for each $r \in R - \{0_R\}$, there exists an $s \in R$ such that $rs = sr = 1_R$). R is a **principal ideal domain (PID)** if every ideal of R is principal; that is, for each ideal $I \subseteq R$, there exists an $r \in R$ such that $I = (r)$.

Part (b): The logical implications among these structures are organized as follows:

$$\text{field} \Rightarrow \text{ED} \Rightarrow \text{PID} \Rightarrow \text{UFD} \Rightarrow \text{ID} \Rightarrow \text{ring} \Rightarrow \text{abelian group}$$

For the final implication, note that by definition a ring is an abelian group under its addition operation (forget the multiplication operation). Each logical implication is strictly one-way. For example, there are euclidean domains that are not fields (for example, the integers).

Part (c): Let $I \subseteq R$ be a nonzero prime ideal, and let $J \subseteq R$ be an ideal such that $I \subseteq J$. We wish to show that $J = I$ or $J = R$. By hypothesis, R is a PID, so there exist $p, m \in R$ such that $I = (p)$ and $J = (m)$. Note that $I \neq (0_R)$ implies $p, m \neq 0_R$. By hypothesis, $p \in I \subseteq J = (m)$, so there exists an $r \in R$ such that

$$p = rm \tag{1}$$

By hypothesis, I is a prime ideal, so $rm = p \in (p) = I$ implies that (i) $r \in I = (p)$ or (ii) $m \in I$. Case (i) implies that there exists an $s \in R$ such that $r = ps$, so by equation (1),

$$p = rm = psm \qquad \Leftrightarrow \qquad p(1_R - sm) = 0_R \qquad \Leftrightarrow \qquad sm = 1_R$$

where the final equivalence follows from the hypothesis that R is a PID (hence an integral domain) and the earlier observation that $p \neq 0_R$. Because J is an ideal, it is strongly closed under multiplication, so $1_R = sm \in (m) = J$. Hence $(1_R) \subseteq J$, so $J = R$. Case (ii) implies that $J = (m) \subseteq I$, hence $J = I$.

Part (d): ($\Leftarrow$) Let R be a field. Then we may define a division algorithm on $R[t]$, which gives $R[t]$ the structure of a euclidean domain. Hence $R[t]$ is a PID. ($\Rightarrow$) Let $R[t]$ be a PID. Then by definition, $R[t]$ is an integral domain, hence the isomorphic image of R in $R[t]$ (namely, the constant polynomials) is an integral domain. Consider the nonzero ideal $(t) \subseteq R[t]$. The quotient $R[t]/(t) \cong R$ is an integral domain, which is equivalent to (t) being a prime ideal. By part (c), it follows that the ideal (t) is maximal, and hence $R \cong R[t]/(t)$ is a field.

Exercise 3

Let t be an indeterminate. We may give $\mathbf{Q}[t]$ the structure of a ring, a $\mathbf{Q}[t]$-module, or a $\mathbf{Z}$-module. For each map below, state whether it is a ring homomorphism, a $\mathbf{Q}[t]$-module homomorphism, or a $\mathbf{Z}$-module homomorphism. Justify your assertions. *Hint:* A given map may satisfy several or none of these conditions.

$$\begin{aligned} \varphi_1 : \mathbf{Q}[t] &\to \mathbf{Q}[t] \\ f(t) &\mapsto 0 \end{aligned} \qquad \begin{aligned} \varphi_2 : \mathbf{Q}[t] &\to \mathbf{Q}[t] \\ f(t) &\mapsto 2f(t) \end{aligned} \qquad \begin{aligned} \varphi_3 : \mathbf{Q}[t] &\to \mathbf{Q}[t] \\ f(t) &\mapsto f(t^2) \end{aligned}$$

Solution: Let $f_1, f_2 \in \mathbf{Q}[t]$. We compute

$$\begin{aligned} \varphi_1(f_1+f_2) &= 0 = 0+0 = \varphi_1(f_1)+\varphi_2(f_2) \\ \varphi_2(f_1+f_2) &= 2(f_1+f_2) = 2f_1+2f_2 = \varphi_2(f_1)+\varphi_2(f_2) \\ \varphi_3(f_1+f_2) &= (f_1+f_2)(t^2) = f_1(t^2)+f_2(t^2) = \varphi_3(f_1)+\varphi_3(f_2) \end{aligned}$$

Thus each map is a homomorphism of abelian groups, which is equivalent to being a $\mathbf{Z}$-module homomorphism.

Next let's check whether each map preserves ring multiplication. We compute

$$\begin{aligned} \varphi_1(f_1f_2) &= 0 = 0 \cdot 0 = \varphi_1(f_1)\varphi_1(f_2) \\ \varphi_2(f_1f_2) &= 2(f_1f_2) \neq 2f_1 \cdot 2f_2 = \varphi_2(f_1)\varphi_2(f_2) \\ \varphi_3(f_1f_2) &= (f_1f_2)(t^2) = f_1(t^2)f_2(t^2) = \varphi_3(f_1)\varphi_3(f_2) \end{aligned}$$

where in the second line we have inequality in general (more precisely, we have equality if and only if f_1 or f_2 is the zero polynomial). Thus φ_2 is not a ring homomorphism. If we define ring homomorphism to map multiplicative identity to multiplicative identity, then φ_1 is not a ring homomorphism (it maps the constant polynomial 1 to 0). If we don't make this restriction in our definition, then φ_1 is a ring homomorphism. For φ_3, our computations for f_1f_2 here and for f_1+f_2 above show that it is a ring homomorphism. Note that $\varphi_3(1) = 1$.

Finally, let's check whether each map preserves the scalar multiplication in a $\mathbf{Q}[t]$-module. (Note that $\mathbf{Q}[t]$ is the ring over which the module is defined, so scalars are elements of $\mathbf{Q}[t]$, not just of $\mathbf{Q}$.) We compute

$$\begin{aligned} \varphi_1(f_1f_2) &= 0 = f_1 \cdot 0 = f_1\varphi_1(f_2) \\ \varphi_2(f_1f_2) &= 2(f_1f_2) = f_1 2f_2 = f_1\varphi_2(f_2) \end{aligned}$$

so φ_1 and φ_2 are $\mathbf{Q}[t]$-module homomorphisms. Taking $f_1 = f_2 = t$, we compute

$$\varphi_3(t \cdot t) = t^4 \neq t \cdot t^2 = t\varphi_3(t)$$

so φ_3 is not a $\mathbf{Q}[t]$-module homomorphism.

We summarize these results in the table below.

Homomorphism of...	φ_1	φ_2	φ_3
$\mathbf{Z}$-modules	Yes	Yes	Yes
$\mathbf{Q}[t]$-modules	Yes	Yes	No
rings	No if we require $1 \mapsto 1$ Yes otherwise	No	Yes

Exercise 4

(a) Let $D_8 = \langle r, s \,|\, r^4, s^2, (rs)^2 \rangle$ be a presentation of the dihedral group of order 8. For each map below, state whether it defines a valid matrix representation of D_8. Justify briefly.

$$\begin{aligned} \rho_1 : D_8 &\to M_2(\mathbf{Q}) \\ r &\mapsto \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \\ s &\mapsto \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \end{aligned} \qquad \qquad \begin{aligned} \rho_2 : D_8 &\to M_2(\mathbf{Q}) \\ r &\mapsto \begin{bmatrix} & 1 \\ -1 & \end{bmatrix} \\ s &\mapsto \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \end{aligned}$$

Now let G be a finite group, let K be a field, and let V be a K-vector space.

(b) Let $\rho : G \to GL(V)$ be a representation of G on V. Explain the induced KG-module structure on V. In particular, specify $(\sum_{g \in G} \alpha_g g) \cdot v$, the ring action of the group ring KG on V.

(c) Define what it means for a module to be (i) decomposable, (ii) reducible, and (iii) completely reducible. (Recall that a representation has one of these properties if the KG-module that affords the representation has that property.)

(d) Further suppose that $\operatorname{char} K \nmid \#G$. Let ρ be a matrix representation of G of degree 2; and let $g_1, g_2 \in G$ such that $\rho(g_1)$ and $\rho(g_2)$ do not commute. Prove that ρ is irreducible.

Solution: Part (a): Recall that, by definition, a (linear) representation is a group homomorphism from a group G to the group of invertible linear transformations of a vector space (or matrix representations thereof); and that to check the conditions of a group homomorphism, it suffices to check that the group relations are satisfied. It is straightforward to check that both maps satisfy the required relations on the generators, namely,

$$\rho_i(r)^4 = I \qquad \rho_i(s)^2 = I \qquad (\rho_i(r)\rho_i(s))^2 = I$$

where I denotes the 2×2 identity matrix.

Part (b): Let $v \in V$; and note that by definition, any element of KG can be expressed as $\sum_{g \in G} \alpha_g g$, where for each $g \in G$, $\alpha_g \in K$. Given a representation $\rho : G \to GL(V)$, the ring action of KG on V is defined by

$$\left(\sum_{g \in G} \alpha_g g \right) \cdot v = \sum_{g \in G} \alpha_g \rho(g)(v)$$

Note that for each $g \in G$, $\rho(g) \in GL(V)$, so $\rho(g)(v) \in V$, so $\alpha_g \rho(g)(v)$ is scalar multiplication of $\alpha_g \in K$ on $\rho(g)(v) \in V$ in the K-vector space V.

Part (c): Let R be a ring, and let M be a nonzero R-module.

1. M is **decomposable** if there exist nonzero submodules $N_1, N_2 \subseteq M$ such that $M = N_1 \oplus N_2$.

2. M is **reducible** if there exists a nonzero proper submodule $N \subseteq M$.

3. M is **completely reducible** if there exist irreducible submodules $N_i \subseteq M$ such that $M = \oplus_i N_i$

Note that, in thje setting of matrix representations φ, these conditions translate as

- decomposable $\Leftrightarrow$ nontrivially block-diagonal
- reducible $\Leftrightarrow$ nontrivally block-upper-triangular

Part (d): Suppose for the sake of contradiction that ρ is reducible. Then by definition, there exists a nonzero proper KG-submodule $N_1 \subseteq V$, where V is the K-vector space underlying the representation ρ. (By hypothesis, $\dim_K V = 2$.) This is equivalent to N_1 being a nonzero proper subspace of V that is G-invariant. Because N_1 is nonzero and proper, it follows that $\dim_K N_1 = 1$. By Maschke's theorem, there exists a submodule $N_2 \subseteq V$ such that $V = N_1 \oplus N_2$. For $i \in \{1, 2\}$, let $v_i \in N_i$ be a nonzero vector; then v_1, v_2 is a basis of V. With respect to this basis (that is, performing a change of basis on the given matrix), the matrix representation of any $g \in G$ is diagonal. In particular, this is true for g_1 and g_2. Because K is a field (hence commutative), it follows that $\rho(g_1)$ and $\rho(g_2)$ commute, a contradiction.

Exercise 5

Let $K : K_0$ be a field extension, let $f \in K_0[t]$, and let $\alpha \in K$.

(a) Briefly explain the difference between viewing f as a polynomial and viewing f as a function. Give two distinct polynomials that define the same function. Justify briefly.

(b) Prove that $f(\alpha) = 0_K$ if and only if $t - \alpha$ divides f in $K[t]$.

(c) Further suppose that $[K : K_0] < \infty$, that f is irreducible in $K_0[t]$, and that $\gcd(\deg f, [K : K_0]) = 1$. Prove that f is irreducible in $K[t]$.

Solution: Part (a): Let $f \in K_0[t]$, say $f = \sum_i a_i t^i$. As a polynomial, f is a formal object. We may view $K_0[t]$ as a (countably) infinite K_0-vector space, and f as the ordered tuple $(a_0, a_1, \ldots)$, where all but finitely many of the a_i equal 0_{K_0}. As a function, f is defined by its domain, codomain, and rule of assignment. The domain and codomain can be any field extension of K_0, including K_0 itself; and the rule of assignment is given by evaluating f at α, that is, $\alpha \mapsto f(\alpha) = \sum_i a_i \alpha^i$.

To illustrate the difference, let $K_0 = \mathbf{F}_2$, the finite field with two elements; and consider $f_1 = 0$ and $f_2 = (t-1)t = t^2 - t$. As polynomials, $f_1 \neq f_2$, because their corresponding coefficients are not all identical. As functions from $\mathbf{F}_2$ to $\mathbf{F}_2$, $f_1 = f_2$: Both are the zero function.

Part (b): ($\Leftarrow$) Let $t - \alpha$ divide f in $K[t]$. Then there exists $g \in K[t]$ such that

$$f(t) = (t - \alpha)g(t)$$

Applying the evaluation homomorphism at $t = \alpha$ to this polynomial equation, we get

$$f(\alpha) = (\alpha - \alpha)g(\alpha) = 0_K$$

($\Rightarrow$) Let $f(\alpha) = 0_K$. Because K is a field, the polynomial ring $K[t]$ is a euclidean domain, with the norm function $N : K[t] \to \mathbf{Z}_{\geqslant 0}$ given by the degree of the polynomial (and the norm of the zero polynomial equal to 0). The polynomial $t - \alpha$ is not the zero element of $K[t]$, so we may divide (with remainder) f by $t - \alpha$: that is, by the division algorithm there exist $q, r \in K[t]$ such that

$$f = (t - \alpha)q + r \tag{2}$$

with $r = 0$ or $\deg r < \deg(t - \alpha) = 1$. Thus r is a constant polynomial. Rewriting this polynomial equation as

$$r = f(t) - (t - \alpha)q(t)$$

and applying the evaluation homomorphism at $t = \alpha$, we get

$$r = f(\alpha) - (\alpha - \alpha)q(\alpha) = 0_K - 0_K = 0_K$$

Substituting this result into equation (2), we conclude that

$$f = (t - \alpha)q$$

so $t - \alpha$ divides f in $K[t]$, as desired.

Part (c): Let θ be a zero of f in some extension field $\tilde{K}$ of K. Consider the composite field $K_0(\theta)K$ in $\tilde{K}$ and the field diagram

$$\begin{tikzcd}
 & K_0(\theta)K \arrow[dl, dash] \arrow[dr, dash] & \\
K_0(\theta) \arrow[dr, dash] & & K \arrow[dl, dash] \\
 & K_0 &
\end{tikzcd}$$

Viewing the composite field $K_0(\theta)K$ as constructed in two stages, along either tower in the diagram, we get[1]

$$[K_0(\theta)K : K_0] \leqslant [K_0(\theta) : K_0][K : K_0] \tag{3}$$

Both $K_0(\theta)$ and K are intermediate fields of $K_0(\theta)K : K_0$, so by the tower law, both $[K_0(\theta) : K_0]$ and $[K : K_0]$ divide $[K_0(\theta)K : K_0]$; hence

$$\operatorname{lcm}([K_0(\theta) : K_0], [K : K_0]) \mid [K_0(\theta)K : K_0]$$

By hypothesis, $\gcd(\deg f, [K : K_0]) = 1$, so

$$\operatorname{lcm}([K_0(\theta) : K_0], [K : K_0]) = [K_0(\theta) : K_0][K : K_0]$$

With the inequality in equation (3), this implies that

$$[K_0(\theta)K : K_0] = [K_0(\theta) : K_0][K : K_0]$$

By the tower law,

$$[K_0(\theta)K : K_0] = [K_0(\theta)K : K][K : K_0]$$

Equating these two expressions for $[K_0(\theta)K : K_0]$ gives an equation in $\mathbf{Z}$, from which we may cancel the common factor of $[K : K_0]$ to get

$$[K_0(\theta)K : K] = [K_0(\theta) : K_0]$$

By definition, the composite field $K_0(\theta)K$ in $\tilde{K}$ is the smallest subfield of $\tilde{K}$ containing $K_0(\theta)$ and K, and $K_0(\theta)$ is the smallest subfield of $\tilde{K}$ containing K_0 and θ. By hypothesis, $K_0 \subseteq K$. Thus $K_0(\theta)K = K(\theta)$. We conclude that

$$\deg m_{\theta,K} = [K(\theta) : K] = [K_0(\theta)K : K] = [K_0(\theta) : K_0] = \deg m_{\theta,K_0} = \deg f$$

Thus f is irreducible in $K[t]$, as desired.

[1] See DF3e, Proposition 13.21, p 529. The key idea is that a basis for a lower extension—$K : K_0$, say—continues to span the "opposite" extension—in this case, $K_0(\theta)K : K_0(\theta)$.

Exercise 6

Let K_0 be a field, let t be an indeterminate, and let $f \in K_0[t]$.

(a) Define what it means for f to be (i) irreducible and (ii) separable. Which of these definitions depends on the polynomial ring in which we consider f? Justify briefly.

Now let $f = t^4 - 4t^2 - 5 \in \mathbf{Q}[t]$.

(b) Show that f is separable and reducible in $\mathbf{Q}[t]$.

(c) Prove that $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) \subseteq \mathbf{C}$ is a splitting field for f over $\mathbf{Q}$.

(d) Prove that $1, \sqrt{5}, \sqrt{-1}, \sqrt{-5}$ is a basis for $\mathbf{Q}(\sqrt{-1}, \sqrt{5})$ as a $\mathbf{Q}$-vector space. Use this basis to specify $\mathrm{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q})$. In particular, show that $\mathrm{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q})$ is generated by two automorphisms, and specify the relations that they satisfy.

Solution: Part (a): K_0 is a field, hence an integral domain, so $K_0[t]$ is an integral domain. Thus the general definition of irreducible applies. That is, let $f \in K_0[t]$ such that $f \neq 0$ and $f \notin (K_0[t])^\times \cong K_0^\times$ (that is, f is not a unit in $K_0[t]$). f is **irreducible** in $K_0[t]$ if for all $f_1, f_2 \in K_0[t]$, if $f = f_1 f_2$, then either f_1 or f_2 is a unit. f is **reducible** if it is not irreducible. In a polynomial ring over a field, this definition is equivalent to saying that f is **reducible** if there exist $f_1, f_2 \in K_0[t]$ such that $f = f_1 f_2$ and for both factors, $\deg f_i < \deg f$.

f is **separable** if each zero of f has multiplicity equal to 1.

The definition of irreducible depends on the polynomial ring in which we consider f. For example, $f = t^2 + 1$ is irreducible in $\mathbf{Q}[t]$ but reducible in $\mathbf{C}[t]$. The definition of separable does not depend on the polynomial ring. Essentially, to assess separability, we pass to a splitting field for f, and all splitting fields for a given polynomial are isomorphic.

Part (b): Note that

$$f = t^4 - 4t^2 - 5 = (t^2 - 5)(t^2 + 1)$$

This shows that f is reducible in $\mathbf{Q}[t]$. It also shows that f has four distinct zeros, $\pm\sqrt{5}$ and $\pm\sqrt{-1}$, in $\mathbf{C}$, so that f is separable.

Part (c): For intuition, a splitting field for f is a "smallest" field that contains all zeros of f, and it can be constructed by taking the field generated by the zeros of f over the base field. More precisely, a splitting field K_f for $f \in \mathbf{Q}[t]$ is a minimal field extension $K_f : \mathbf{Q}$ such that f factors completely into linear factors in $K_f[t]$; by "minimal", we mean for any field K such that $K_f : K : \mathbf{Q}$, if f factors completely into linear factors in $K[t]$, then $K = K_f$.

By construction and the fact that fields are closed under the field operations (including taking additive inverses), $\mathbf{Q}(\sqrt{-1}, \sqrt{5})$ contains all four zeros of f, and it contains $\mathbf{Q}$. This shows that $\mathbf{Q}(\sqrt{-1}, \sqrt{5})$ contains a splitting field for f over $\mathbf{Q}$. By definition, any splitting field for f over $\mathbf{Q}$ in $\mathbf{C}$ contains $\mathbf{Q}$, $\sqrt{-1}$, and $\sqrt{5}$, and hence contains $\mathbf{Q}(\sqrt{-1}, \sqrt{5})$. This shows that $\mathbf{Q}(\sqrt{-1}, \sqrt{5})$ is minimal, as defined above.

Part (d): Consider constructing $\mathbf{Q}(\sqrt{-1}, \sqrt{5})$ in two steps. First, adjoin $\sqrt{5}$ to $\mathbf{Q}$ to get $\mathbf{Q}(\sqrt{5})$. Note that

$$[\mathbf{Q}(\sqrt{5}) : \mathbf{Q}] = \deg m_{\sqrt{5},\mathbf{Q}} = \deg(t^2 - 5) = 2$$

so a basis for $\mathbf{Q}(\sqrt{5})$ as a $\mathbf{Q}$-vector space is $\mathcal{B}_1 = 1, \sqrt{5}$. Moreover, $\mathbf{Q}(\sqrt{5})$ is a subfield of $\mathbf{R}$, so in particular it does not contain $\pm\sqrt{-1}$. Because the minimal polynomial of $\sqrt{-1}$ over $\mathbf{Q}$ has degree 2, it must remain the minimal polynomial of $\sqrt{-1}$ over $\mathbf{Q}(\sqrt{5})$:

$$m_{\sqrt{-1},\mathbf{Q}(\sqrt{5})} = m_{\sqrt{-1},\mathbf{Q}} = t^2 + 1$$

Second, adjoin $\sqrt{-1}$ to $\mathbf{Q}(\sqrt{5})$ to get $(\mathbf{Q}(\sqrt{5}))(\sqrt{-1}) \cong \mathbf{Q}(\sqrt{-1}, \sqrt{5})$. A basis for $\mathbf{Q}(\sqrt{-1}, \sqrt{5})$ as a $\mathbf{Q}(\sqrt{5})$-vector space is $\mathcal{B}_2 = 1, \sqrt{-1}$. Taking all pairwise products of elements in $\mathcal{B}_1$ and $\mathcal{B}_2$ gives a basis $\mathcal{B}$ for $\mathbf{Q}(\sqrt{-1}, \sqrt{5})$ as a $\mathbf{Q}$-vector space

$$\mathcal{B} = 1, \sqrt{5}, \sqrt{-1}, \sqrt{-5}$$

Note that, by definition

$$[\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}] = \dim_{\mathbf{Q}} \mathbf{Q}(\sqrt{-1}, \sqrt{5}) = \#\mathcal{B} = 4$$

We can also see this using the tower law:

$$\begin{aligned}
[\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}] &= [\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}(\sqrt{5})][\mathbf{Q}(\sqrt{5}) : \mathbf{Q}] \\
&= \deg m_{\sqrt{-1},\mathbf{Q}(\sqrt{5})} \cdot \deg m_{\sqrt{5},\mathbf{Q}} \\
&= 2 \cdot 2 = 4
\end{aligned}$$

An automorphism $\sigma \in \operatorname{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q})$ is completely determined by where it sends the generators $\sqrt{-1}$ and $\sqrt{5}$ of the field extension; and it must send each to a zero of its minimal polynomial over the base field, $\mathbf{Q}$. Thus

$$\sigma(\sqrt{-1}) = \pm\sqrt{-1} \qquad\qquad \sigma(\sqrt{5}) = \pm\sqrt{5}$$

This gives a maximum of four candidate automorphisms. One can check directly that each candidate indeed defines a valid automorphism of $\operatorname{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q})$. Alternatively, one can argue indirectly that the field extension $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}$ is galois (see Exercise 7(a)), and therefore $\# \operatorname{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}) = [\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}] = 4$, so that each candidate must be in $\operatorname{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q})$.

Let

$$\begin{aligned}
\sigma_{-1} : \mathbf{Q}(\sqrt{-1}, \sqrt{5}) &\to \mathbf{Q}(\sqrt{-1}, \sqrt{5}) \\
\sqrt{-1} &\mapsto -\sqrt{-1} \\
\sqrt{5} &\mapsto \sqrt{5}
\end{aligned}
\qquad\qquad
\begin{aligned}
\sigma_5 : \mathbf{Q}(\sqrt{-1}, \sqrt{5}) &\to \mathbf{Q}(\sqrt{-1}, \sqrt{5}) \\
\sqrt{-1} &\mapsto \sqrt{-1} \\
\sqrt{5} &\mapsto -\sqrt{5}
\end{aligned}$$

It is straightforward to check that

$$\operatorname{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}) = \langle \sigma_{-1}, \sigma_5 \,|\, \sigma_{-1}^2, \sigma_5^2, (\sigma_{-1}\sigma_5)^2 \rangle$$

Exercise 7

We continue to consider the polynomial $f = t^4 - 4t^2 - 5 \in \mathbf{Q}[t]$ from Exercise 6.

(a) Give two distinct arguments that the field extension $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}$ is galois.

(b) Draw a diagram of subgroups of $\operatorname{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q})$ and a diagram of subfields (intermediate fields) of $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}$. Clearly indicate the galois correspondences.

(c) Let $\alpha = \sqrt{-1} + \sqrt{5} \in \mathbf{C}$. Prove that $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{-1}, \sqrt{5})$. *Hint:* Consider α^{-1}.

(d) Find the minimal polynomial $m_{\alpha,\mathbf{Q}}$ of α over $\mathbf{Q}$. Justify that it satisfies all defining axioms of a minimal polynomial.

Solution: Part (a): We have several equivalent characterizations of a galois extension.

1. If we checked directly that the four maps in our response to Exercise 6(d) were valid automorphisms of $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}$, then $\# \operatorname{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}) = [\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}]$, which is what we took as the definition of a galois extension in our development of the theory.

2. In Exercise 6(c) we showed that $\mathbf{Q}(\sqrt{-1}, \sqrt{5})$ is a splitting field for f over $\mathbf{Q}$, and in Exercise 6(b) we showed that f is separable. Thus $\mathbf{Q}(\sqrt{-1}, \sqrt{5})$ is a splitting field for a separable polynomial in $\mathbf{Q}[t]$, which is equivalent to $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}$ being galois.

3. If we compute the fixed field for the full automorphism group, then we find

$$\mathcal{F}(\operatorname{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q})) = \mathbf{Q}$$

the original base field, which is equivalent to $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}$ being galois.

Part (b): The subfield and subgroup diagrams are

$$\begin{tikzcd}
 & \mathbf{Q}(\sqrt{-1}, \sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbf{Q}(\sqrt{-1}) \arrow[dr, dash] & \mathbf{Q}(\sqrt{-5}) \arrow[d, dash] & \mathbf{Q}(\sqrt{5}) \arrow[dl, dash] \\
 & \mathbf{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \{\mathrm{id}_{\mathbf{Q}(\sqrt{-1}, \sqrt{5})}\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \sigma_5 \rangle \arrow[dr, dash] & \langle \sigma_{-1}\sigma_5 \rangle \arrow[d, dash] & \langle \sigma_{-1} \rangle \arrow[dl, dash] \\
 & \langle \sigma_{-1}, \sigma_5 \rangle &
\end{tikzcd}$$

In these two diagrams, algebraic objects in corresponding positions correspond by the galois correspondence, namely

$$\begin{aligned} K_i &\mapsto \operatorname{Aut}(K : K_i) \\ \mathcal{F}(H_i) &\mapsfrom H_i \end{aligned}$$

where we denote $K = \mathbf{Q}(\sqrt{-1}, \sqrt{5})$.

Part (c): Observe that $\alpha = \sqrt{-1} + \sqrt{5} \in \mathbf{Q}(\sqrt{-1}, \sqrt{5})$ (because fields are closed under the field operations), so

$$\mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\sqrt{-1}, \sqrt{5})$$

For the reverse inclusion, note that

$$\alpha^{-1} = \frac{1}{\sqrt{-1} + \sqrt{5}} = \frac{\sqrt{-1} - \sqrt{5}}{-1 - 5} = -\frac{1}{6}\sqrt{-1} + \frac{1}{6}\sqrt{5}$$

Again, fields are closed under the field operations (including taking additive and multiplicative inverses), so the field $\mathbf{Q}(\alpha)$ contains α^{-1} and hence also

$$\sqrt{5} = \frac{1}{2}(\alpha + 6\alpha^{-1}) \qquad \text{and} \qquad \sqrt{-1} = \alpha - \sqrt{5}$$

so $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) \subseteq \mathbf{Q}(\alpha)$. Together, these inclusions show that $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) = \mathbf{Q}(\alpha)$, as desired.

Part (d): Starting with the defining equation for α, we successively isolate radicals and take powers to get an equation involving only α and the desired base field $\mathbf{Q}$:

$$\begin{aligned} \alpha = \sqrt{-1} + \sqrt{5} \quad &\Rightarrow \quad (\alpha - \sqrt{5})^2 = -1 \quad &\Leftrightarrow \quad \alpha^2 + 6 = 2\sqrt{5}\alpha \\ &\Rightarrow \quad (\alpha^2 + 6)^2 = 20\alpha^2 \quad &\Leftrightarrow \quad \alpha^4 - 8\alpha^2 + 36 = 0 \end{aligned}$$

Viewing this last equation as a polynomial evaluated at $t = \alpha$, we define

$$f = t^4 - 8t^2 + 36$$

By construction, $f(\alpha) = 0$, and by inspection, f is monic. To show that $f = m_{\alpha,\mathbf{Q}}$, it remains only to show that f is irreducible. One way to show this is to use Exercises 6(d) (which implies that $[\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}] = 4$) and 7(c) (which shows that $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{-1}, \sqrt{5})$):

$$\deg m_{\alpha,\mathbf{Q}} = [\mathbf{Q}(\alpha) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}] = 4$$

The fact that $f(\alpha) = 0$ implies that $m_{\alpha,\mathbf{Q}} \mid f$, say $f = g m_{\alpha,\mathbf{Q}}$. Both $m_{\alpha,\mathbf{Q}}$ and f have degree 4, so (using the fact that $\mathbf{Q}[t]$ is an integral domain, because $\mathbf{Q}$ is)

$$\deg f = \deg(g m_{\alpha,\mathbf{Q}}) = \deg g + \deg m_{\alpha,\mathbf{Q}} \qquad \Leftrightarrow \qquad \deg g = \deg f - \deg m_{\alpha,\mathbf{Q}} = 0$$

Thus $g \in \mathbf{Q}[t]$ is a nonzero constant, hence a unit. Because $m_{\alpha,\mathbf{Q}}$ is irreducible by definition of minimal polynomial, and $f = g m_{\alpha,\mathbf{Q}}$, we conclude that f is irreducible.

Exercise 8

This exercise, combined with the theory of solvable groups, shows that the general quintic (and hence the general polynomial of degree $n \geqslant 5$) cannot be solved by radicals.

Let $f = t^5 - 6t + 3 \in \mathbf{Q}[t]$, and let $K_f \subseteq \mathbf{C}$ be the splitting field for f in $\mathbf{C}$.

(a) Prove that f is irreducible in $\mathbf{Q}[t]$. Deduce that $5 \mid [K_f : \mathbf{Q}]$.

(b) Prove that f has exactly three zeros in $\mathbf{R}$ and exactly two zeros in $\mathbf{C} - \mathbf{R}$. You may use the values in the table below in your proof.

t	-2	-1	0	1	2
$f(t)$	-17	8	3	-2	23
$f'(t)$	74	-1	-6	-1	74

(c) Let $\tau_{\mathbf{C}} : \mathbf{C} \to \mathbf{C}$ denote the automorphism of $\mathbf{C}$ of complex conjugation (that is, for all $a, b \in \mathbf{R}$, $\tau_{\mathbf{C}}(a + bi) = a - bi$), and let $\tau \in \operatorname{Aut}(K_f : \mathbf{Q})$ be the restriction of $\tau_{\mathbf{C}}$ to K_f. Prove that τ fixes the three real zeros of f and swaps the two non-real complex ones.

(d) Justify why $K_f : \mathbf{Q}$ is galois. Deduce that $\operatorname{Gal}(K_f : \mathbf{Q}) \cong S_5$, the symmetric group on five elements. *Hint:* You may use without proof the fact that S_5 is generated by $\{\sigma_2, \sigma_5\}$, where $\sigma_m \in S_5$ is an m-cycle.

Solution: Part (a): View $f \in \mathbf{Z}[t]$. Then the Eisenstein–Schönemann criterion with prime $p = 3$ applies to f: 3 does not divide the leading coefficient, 3 divides all other coefficients, and 3^2 does not divide the constant term. Thus f is irreducible in $\mathbf{Z}[t]$. Gauß's lemma then implies that f is irreducible in $\mathbf{Q}[t]$.

To show that $5 \mid [K_f : \mathbf{Q}]$, consider constructing the splitting field K_f for f in $\mathbf{C}$ by starting from $\mathbf{Q}$ and adjoining one zero of f at a time. Let $\alpha_1, \ldots, \alpha_5$ be the zeros of f in $\mathbf{C}$,[2] and recall that $K_f = \mathbf{Q}(\alpha_1, \ldots, \alpha_5)$. Then by the tower law,[3]

$$[K_f : \mathbf{Q}] = [\mathbf{Q}(\alpha_1, \ldots, \alpha_5) : \mathbf{Q}] = [\mathbf{Q}(\alpha_1, \ldots, \alpha_4)(\alpha_5) : \mathbf{Q}(\alpha_1, \ldots, \alpha_4)] \cdots [\mathbf{Q}(\alpha_1) : \mathbf{Q}] \tag{4}$$

Because α_1 is a zero of f and f is irreducible (in fact, f is the minimal polynomial of each α_m over $\mathbf{Q}$), we have

$$[\mathbf{Q}(\alpha_1) : \mathbf{Q}] = \deg m_{\alpha_1, \mathbf{Q}} = \deg f = 5$$

Thus equation (4) implies that $5 \mid [K_f : \mathbf{Q}]$, as desired.

Part (b): View $f \in \mathbf{Q}[t]$ as a function $f : \mathbf{R} \to \mathbf{R}$. Because the rule of assignment for this function is a polynomial, the function is continuous. Thus the intermediate value theorem applies: From

[2] A priori, a polynomial might have repeated zeros, but we know f does not. Why?

[3] To simplify notation, for $m \in \{0, \ldots, 5\}$, let $K_m = \mathbf{Q}(\alpha_1, \ldots, \alpha_m)$, with the convention that $K_0 = \mathbf{Q}$. Then for each $m \in \{1, \ldots, 5\}$, $K_m = K_{m-1}(\alpha_m)$, and equation (4) writes as

$$[K_5 : K_0] = [K_5 : K_4] \cdots [K_1 : K_0]$$

the table of values of $f(t)$, we see that f has zeros on the intervals $(-2,-1)$, $(0,1)$, and $(1,2)$. Thus f has at least three real zeros. To show that f has at most three real zeros, consider the derivative

$$f' = D_t f = 5t^4 - 6$$

viewed as a function $\mathbf{R} \to \mathbf{R}$. If f had four real zeros, then the sign of $f'(t)$ would have to change at least four times, so by the intermediate value theorem, f' would have at least three real zeros. However, f' has precisely two real zeros, both of multiplicity one. By the fundamental theorem of algebra, f has $\deg f = 5$ zeros in $\mathbf{C}$, and we have shown that exactly three of them are real, so we conclude that f has exactly two zeros in $\mathbf{C} - \mathbf{R}$.

Alternatively, one can use Descartes's rule of signs: Let $g \in \mathbf{R}[t]$, say $g = a_n t^n + \ldots + a_0$, with $a_n \neq 0$. (For simplicity, omit terms with a zero coefficient.) Then the number of positive real zeros of g, counted with multiplicity, equals the number of sign changes of the coefficients of $g(t)$, minus $2k$ for some $k \in \mathbf{Z}_{\geqslant 0}$. As a corollary, the number of negative real zeros of g, counted with multiplicity, equals the number of sign changes of the coefficients of $g(-t)$, minus $2k$ for some $k \in \mathbf{Z}_{\geqslant 0}$. Applying this to f,

$$f(t) = t^5 - 6t + 3 \qquad\qquad f(-t) = -t^5 + 6t + 3$$

we get that f has either 0 or 2 positive real zeros, and exactly 1 negative real zero. Because $f(0) = 3 \neq 0$, it follows that f has exactly 1 or 3 real zeros. The table of values of $f(t)$ and the intermediate value theorem allow us to distinguish these cases and conclude that exactly 3 real zeros. It follows that the other two zeros of f in $\mathbf{C}$ guaranteed by the fundamental theorem of algebra must be nonreal.

Part (c): Because the coefficients of f are in $\mathbf{Q} \subseteq \mathbf{R}$, any complex zeros of f must come in complex conjugate pairs. We have shown that f has exactly two nonreal complex zeros, so they must be complex conjugates, and are therefore swapped by τ. Because $\tau_{\mathbf{C}}$ fixes $\mathbf{R}$, it follows that τ fixes the real zeros of f.

Part (d): K_f is a splitting field for $f \in \mathbf{Q}[t]$, and f is separable,[4] so $K_f : \mathbf{Q}$ is galois. Hence[5]

$$\#\mathrm{Gal}(K_f : \mathbf{Q}) = [K_f : \mathbf{Q}] \leqslant (\deg f)! = 5!$$

In part (a) we showed that $5 \,|\, [K_f : \mathbf{Q}]$. It follows that $\#\mathrm{Gal}(K_f : \mathbf{Q}) = 5q$, where $q \in \mathbf{Z}$ is not divisible by 5. By the Sylow theorems, $\mathrm{Gal}(K_f : \mathbf{Q})$ contains a Sylow 5-subgroup, which must contain an element of order 5. The only elements in S_5 of order 5 are 5-cycles, so $\mathrm{Gal}(K_f : \mathbf{Q})$

[4] We can prove that f is separable in various ways:

1. Our analysis of the zeros of f proves it from the definition: In part (b) we showed that f has three distinct real zeros, and our work in parts (b) and (c) showed that f has two distinct nonreal complex zeros. Thus all the zeros of f are distinct.

2. Alternatively, by part (a), $f \in \mathbf{Q}[t]$ is irreducible; and the field of coefficients, $\mathbf{Q}$, is perfect (implied by $\mathrm{char}\,\mathbf{Q} = 0$). Therefore f is separable.

[5] The first equality uses the fact that $K_f : \mathbf{Q}$ is galois. The inequality uses the theory of splitting fields: Think of the "worst-case" scenario when constructing a splitting field of f by adjoining one zero at a time. Another way to see the inequality is to argue directly on $\mathrm{Gal}(K_f : \mathbf{Q})$: An automorphism in the galois group must send a zero of a polynomial to another (possibly the same) zero of that polynomial. That is, automorphisms in the galois group permute the zeros of a polynomial defined over the base field. Moreover, an automorphism in the galois group is completely determined by its action on the generators of the extension field; here, $K_f = \mathbf{Q}(\alpha_1, \ldots, \alpha_5)$, where $\{\alpha_1, \ldots, \alpha_5\}$ is the set of (five) distinct zeros of f in K_f. From this, we conclude that $\mathrm{Gal}(K_f : \mathbf{Q})$ is a subgroup of S_5.

contains a 5-cycle. In part (c) we showed that $\tau \in \mathrm{Gal}(K_f : \mathbf{Q})$ swaps the two nonreal complex zeros and fixes the other zeros of f, so τ is a 2-cycle. We now appeal to the conveniently provided fact that a subgroup of S_5 that contains a 2-cycle and a 5-cycle is necessarily the whole group S_5 to conclude that $\mathrm{Gal}(K_f : \mathbf{Q}) \cong S_5$.